

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATE

REMARKS

The following Remarks are made in response to the Office Action mailed November 28, 2003. Claims 1-24 were rejected. With this Response, claims 1, 10-13, and 22-24 have been amended. Claims 1-24 remain pending in the application and are presented for reconsideration and allowance.

Informalities

The Examiner objected to the specification because corrected patent application numbers are required for the related applications listed on page 1. The specification has been amended to update the Cross Referenced to Related Applications paragraph with patent application serial numbers. Withdrawal of the objections to the specification is respectfully requested.

Claim Rejections under 35 U.S.C. § 112

The Examiner rejected claims 1-24 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Examiner states that a “public key certificate” was defined in the specification as a digital document that includes a signature of a certificate authority. As a result, the Examiner concluded that the term “unsigned certificate” of claims 1 and 13 is indefinite. Applicant notes this apparent contradiction with appreciation and, with this Amendment and Response, submits a clarification to the specification to resolve the apparent contradiction.

In particular, the definition of a “public key certificate” appearing in the Background of the Invention section of the application beginning on page 2, line 9, has been clarified to refer to a *traditional* public key certificate. In view of this clarification, Applicant respectfully submits that pending claims 1-24 are definite and in conformance with the requirements of 35 U.S.C. § 112, second paragraph.

Furthermore, Applicant respectfully points out that the clarification made is consistent with other parts of the present application. For example, in the present specification beginning at page 9, line 3, states, “In contrast to the traditional long-term certificates employed by conventional PKIs, the *unsigned certificates* for authentication of subject 34 to

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATE

verifier 36 according to the present invention *are not signed*, do not need an expiration date, and do not use CRLs.” Applicant respectfully submits that since the clarification is consistent with the claims and the other parts of the present specification the clarification is not adding new matter.

In view of the above, Applicant respectfully requests withdrawal of the § 112 rejection of claims 1-24.

Claim construction

Due to the apparent contradiction noted by the Examiner between the definition of “public key certificate” appearing in the Background of the Invention section of the present patent application and the claim language, the Examiner interpreted the term “unsigned” to mean that the certificate is only signed by the certificate authority for the application.

In view of the clarification to the specification described above, Applicant respectfully submits that there is no contradiction between the claim language and the specification. Therefore, Applicant respectfully points out that the language of claims 1-24 should be interpreted according to its plain meaning and in light of the specification in its entirety (e.g., the specification at page 9, lines 4-6 states “the unsigned certificates for authentication of subject 34 to verifier 36 according to the present invention are not signed”). In particular, the “unsigned certificate” term in independent claims 1 and 13 is defined in the claims as a certificate that “binds a public key of the subject to long-term identification information related to the subject.” Since, in claims 1 and 13, the unsigned certificate is recited as being “unsigned,” Applicant respectfully submits that “unsigned certificate” should be interpreted to refer to a certificate that binds a public key of the subject to long-term identification information related to the subject, and that is not signed by the issuing certificate authority.

Claim Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1, 2, 6, 7, 8, 13, 14, and 18-20 under 35 U.S.C. § 102(e) as being anticipated by Andrews (U.S. Patent No. 6,324,645).

The Andrews patent describes a public key management infrastructure for managing risks associated with the use of public key certificates in a public key infrastructure. Digital

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATE

certificates are issued and signed by a certificate authority. A public key management infrastructure stores digital certificates issued to users, and coupled with a security engine that permits user access to the certificates only after certain authenticating or authorizing conditions are met.

Applicant respectfully submits that the Andrews patent fails to teach or suggest every limitation claimed in independent claims 1 and 13. For example, the Andrews patent does not teach or suggest unsigned certificates. Throughout the specification and claims of the Andrews patent, digital certificates are characterized as being signed by the issuing certificate authority (CA). For instance, the abstract of the Andrews patent states, "The user (102) is associated (301) with a digital certificate (200) which is issued *and digitally signed by a certification authority* (CA)." By contrast, independent claims 1 and 13 include the limitations of *unsigned* certificates, and respectively claim a public key infrastructure (PKI) and method of authenticating a subject to a verifier in a PKI using unsigned certificates. The Andrews patent does not teach or suggest unsigned certificates or the use of unsigned certificates.

Claims 1 and 13 further includes limitations of the verifier maintaining a hash table containing cryptographic hashes of valid unsigned certificates. In contrast, the Andrews patent describes the use of hash functions (e.g., generating a "message digest" by applying a hash function to a digital certificate prior to signing it, or as part of verifying the certificate). The Andrews patent also describes maintaining database records including "jurisdiction hashes" at the public key management infrastructure. A "jurisdiction hash" is defined in the Andrews patent beginning at col. 9, line 59, as a "one-way hash of the organization name." A jurisdiction hash is an embodiment of an "access label," which is a part of a digital certificate (see, e.g., reference number 216 in Figure 2). Consequently, the Andrews patent does not teach or suggest maintaining a hash table by the verifier containing cryptographic hashes of *valid unsigned certificates*, as recited in independent claims 1 and 13.

In view of the above, Applicant respectfully submits that the Andrews patent does not teach or suggest every limitation claimed in independent claims 1 and 13. As dependent claims 2 and 6-8 further define patentably distinct independent claim 1, and as dependent claims 14 and 18-20 further define patentably distinct independent claim 13, these dependent claims are also believed to be allowable. Therefore, Applicant respectfully requests

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATE

reconsideration and withdrawal of the § 102 rejection to claims 1-2, 6-8, 13-14, and 18-20 and allowance of these claims.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected claims 3-4, and 15-16 under 35 U.S.C. § 103(a) as being unpatentable over the Andrews U.S. Patent No. 6,324,645 in view of the Maruyama U.S. Patent No. 6,393,563.

The Examiner rejected claims 5 and 17 under 35 U.S.C. § 103(a) as being unpatentable over the Andrews U.S. Patent No. 6,324,645 in view of the Kausik U.S. Patent No. 6,263,446.

The Examiner rejected claims 9 and 21 under 35 U.S.C. § 103(a) as being unpatentable over the Andrews U.S. Patent No. 6,324,645 in view of the Gasser U.S. Patent No. 5,224,163.

The Examiner rejected claims 10-11 and 22-23 under 35 U.S.C. § 013(a) as being unpatentable over the Andrews U.S. Patent No. 6,324,645 in view of the Micali U.S. Patent No. 5,793,868 in view of the Boyle U.S. Patent No. 6,212,636.

The Examiner rejected claims 12 and 24 under 35 U.S.C. § 013(a) as being unpatentable over the Andrews U.S. Patent No. 6,324,645 in view of Micali U.S. Patent No. 5,793,868 in view of the Boyle U.S. Patent No. 6,212,636 in view of the Gasser U.S. Patent No. 5,224,163.

In view of the above, independent claims 1 and 13 are believed to be allowable. As dependent claims 3-5 and 9-12 further define patentably distinct independent claim 1; and as dependent claims 15-17 and 21-24 further define patentably distinct independent claim 13, these dependent claims are also believed to be allowable. Therefore, Applicant respectfully requests that the § 103 rejections to claims 3-5, 9-12, 15-17, and 21-24 be removed and that these claims be allowed.

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-24 are in form for allowance and are not taught or suggested by the cited references. Therefore,

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/483,186

Filed: January 14, 2000

Docket No.: 10001559-1

Title: LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATE

reconsideration and withdrawal of the rejections and allowance of claims 1-24 is respectfully requested.

No fees are required under 37 C.F.R. 1.16(b)(c). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 08-2025.

The Examiner is invited to contact either the Applicant's Representative at the below-listed telephone number or William J. Streeter, Esq. at Telephone No. (970) 898-3886, Facsimile No. (970) 898-7247 to facilitate prosecution of this application. In addition, all correspondence should continue to be directed to the following address:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

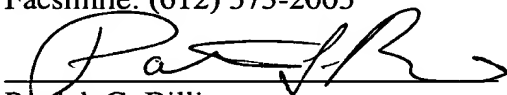
Respectfully submitted,

Francisco Corella

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Date: March 1, 2004
PGB:vb:mad


Patrick G. Billig
Reg. No. 38,080

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, as first class mail, in an envelope address to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 1st day of March, 2004

By 
Name: Patrick G. Billig